Conspectus materiae tomi XLIV, fasciculi 1

La revue est consacrée à la Théorie des Nombres
The journal publishes papers on the Theory of Numbers
Die Zeitschrift veröffentlicht Arbeiten aus der Zahlentheorie
Журнал посвящен теории чисел

L'adresse de la Rédaction et de l'échange | Address of the Editorial Board and of the exchange | Die Adresse der Schriftleitung und des Austausches | Адрес редакции и книгообмена

ACTA ARITHMETICA
ul. Śniadeckich 8, 00-950 Warszawa

Les auteurs sont priés d'envoyer leurs manuscrits en deux exemplaires
The authors are requested to submit papers in two copies
Die Autoren sind gebeten um Zusendung von 2 Exemplaren jeder Arbeit
Рукописи статей редакция просит предлагать в двух экземплярах

ISBN 83-01-05223-6 ISSN 0065-1036

PRINTED IN POLAND

W R O C Ł A W S K A D R U K A R N I A N A U K O W A

ACTA ARITHMETICA
XLIV (1984)

Sequences of integers whose iterated sums are disjoint

by

JOHN R. BURKE and WILLIAM A. WEBB (Pullman, Wash.)

1. Introduction. If A and B are sets of nonnegative integers we write $A+B = \{n\colon n = a+b,\ a\in A,\ b\in B\}$. Erdös and Sárközy [1] studied the conditions under which $A+A\cap B\neq\emptyset$. It is natural to ask in some sense how dense sets can be and still be disjoint. In the case mentioned above, once A is chosen, by taking B to be the complement of $A+A$ we get a relatively dense example. In particular if $A=\{n\colon n\equiv 0 \pmod 2\}$ and $B=\{n\colon n\equiv 1 \pmod 2\}$, $A+A\cap B=\emptyset$, A and B are equally dense (in the asymptotic sense), and $A\cup B$ contains all nonnegative integers. This serves naturally as an example of maximum density.

In this paper we consider the problem of characterizing maximal examples of sets A and B such that $A+A\cap B+B=\emptyset$ (as well as the more general problem of higher order sums being disjoint).

DEFINITION 1. Two sets of nonnegative integers A and B are *sum disjoint* if $A+A\cap B+B=\emptyset$.

As usual, the lower asymptotic density of a set A is defined to be $\underline{d}(A) = \liminf A(n)/n$, where $A(n)$ is the number of positive elements of A not exceeding n.

The main result concerning sum disjoint sets is:

THEOREM 1. *If A and B are infinite sum disjoint sets of nonnegative integers and $\underline{d}(A)\leqslant\underline{d}(B)$, then either*

(i) $\underline{d}(A)=0$ *and* $\underline{d}(B)\leqslant 1/2$

or

(ii) *there exists a positive integer k such that*

$$\underline{d}(A)\leqslant\frac{1}{2k+1}\quad\text{and}\quad\underline{d}(B)\leqslant\frac{k}{2k+1}.$$

2. Proof of Theorem 1. Before proving Theorem 1 we will need a number of definitions and lemmas. Some of this terminology is due to M. Kneser [2], [4], [5].

DEFINITION 2. A is said to be *degenerate* (mod g) if A is the union of entire congruence classes (mod g). A is said to be *essentially degenerate* (mod g) if A is contained in a sequence B which is degenerate (mod g) and $\underline{d}(A) = \underline{d}(B)$. (That is, $A \cup C$ is degenerate (mod g) for some set C, $\underline{d}(C) = 0$.)

DEFINITION 3. A' is said to be *g-worse than* A if A' is degenerate (mod g) and

(i) $A \subset A'$,

(ii) $A+A = A'+A'$ from some point on.

If we choose $A = \{n\colon n \equiv 0 \pmod 3,\ n \geqslant 0\}$ and $B = \{n\colon n \equiv 1 \pmod 3,\ n \geqslant 0\}$, it is clear that A and B are sum disjoint. It may also be noted that the only sequence which is 3-worse than A is A itself, similarly for B.

As a special case of Kneser's theorem on sums of sequences we have the following:

THEOREM 2 (Kneser [2], [4]). *Let A be a sequence of nonnegative integers and let h be a positive integer. Then either*

(1) $$\underline{d}(hA) \geqslant h\underline{d}(A), \quad \text{where} \quad hA = \{n\colon n = \sum_{i=1}^{h} a_i,\ a_i \in A\}$$

or

(2) *there exists a sequence A' which is g-worse than A.*

Suppose A and B are sum disjoint, and both satisfy (1). We may assume $\underline{d}(A) \leqslant \underline{d}(B)$. Then either $\underline{d}(A) = 0$ and $\underline{d}(B) \leqslant 1/2$ or there exists a positive integer k such that $1/(2k+3) < \underline{d}(A) \leqslant 1/(2k+1)$. Since A and B are sum disjoint, $\underline{d}(B) \leqslant 1/2 - 1/(2k+3) \leqslant k/(2k+1)$, so Theorem 1 holds. We now assume that at least one of the sequences must satisfy (2).

If A satisfies (2), then there exists a sequence A' which is g-worse than A for some integer g. Since $A'+A' = A+A$ from some point on, by deleting at most a finite number of elements from B we obtain a new sequence B' such that A' and B' are sum disjoint. Since B' differs from B by only a finite set it follows that $\underline{d}(B) = \underline{d}(B')$. Similarly, since $A \subset A'$, we have $\underline{d}(A') \geqslant \underline{d}(A)$. Thus we may assume A is degenerate (mod g).

LEMMA 1. *Let A and B be sum disjoint. If A is degenerate* (mod g) *then there exists a sequence B' such that*

(i) *B' is degenerate* (mod g),

(ii) $\underline{d}(B) \leqslant \underline{d}(B')$,

(iii) *A and B' are sum disjoint.*

Proof. Let A be degenerate (mod g). Define $B' = \{n\colon n \geqslant 0;$ and $\exists\, b \in B,\ b \geqslant g,\ n \equiv b \pmod g\}$. Thus B' is degenerate (mod g).

If $b \in B$ and $b \geqslant g$, then $b \in B'$. It follows that $\underline{d}(B) \leqslant \underline{d}(B')$.

Assume $c \in (A+A) \cap (B'+B')$. Then there exists $a_1, a_2 \in A$ and $b_1', b_2' \in B'$ such that $c = a_1 + a_2 = b_1' + b_2'$. From the definition of B' there are elements $b_1, b_2 \in B$ such that $b_1 \geqslant g$, $b_2 \geqslant g$, $b_1 \equiv b_1' \pmod g$ and $b_2 \equiv b_2' \pmod g$. Since A is degenerate (mod g) it follows that $A+A$ is essentially degenerate (mod g), missing perhaps the least element in any given residue class (mod g) which is represented in $A+A$. Hence, $b_1 \geqslant g$, $b_2 \geqslant g$, and $a_1 + a_2 \equiv b_1 + b_2 \pmod g$ implies that $b_1 + b_2 \in A+A$. This contradicts the assumption that A and B are sum disjoint. Thus A and B' are also sum disjoint.

In light of Lemma 1 it may be assumed that the sum disjoint sequences A and B which maximize $\underline{d}(A) + \underline{d}(B)$ are degenerate (mod g) for some g, and so addition of the sequences A and B may be viewed as the addition of residue classes (mod g).

Let Z_g denote the additive group of residues (mod g). If $\mathscr{A} \subset Z_g$, then denote the number of elements (residue classes (mod g)) in $\mathscr{A}$ by $[\mathscr{A}]$. If $\mathscr{A} \subset Z_g$, then denote the subgroup of Z_g which leaves $\mathscr{A}$ invariant by $H(\mathscr{A})$. That is, $a \in H(\mathscr{A})$ if and only if $a + \mathscr{A} = \mathscr{A}$. If $[H(\mathscr{A})] \geqslant 2$, then we say $\mathscr{A}$ is periodic ([3]).

Let C be a degenerate sequence (mod g) and let $\bar{C}$ denote the set of residues (mod g) represented by some element of C. Thus $\bar{C} \subset Z_g$. If A is degenerate (or essentially degenerate) and $\bar{C}$ is periodic, then we say C is periodic (mod g).

LEMMA 2. *If A is degenerate* (mod g) *and $\bar{A}+\bar{A}$ is periodic, then $A+A$ is essentially degenerate* (mod k) *for some positive integer $k < g$ such that $k|g$.*

Proof. $H(\bar{A}+\bar{A}) = H$ is a subgroup of Z_g and hence cyclic. If k is the least positive integer which, considered as an element of H, generates H, then $k|g$, and since $[H] \geqslant 2$ we have $k < g$.

Let $r \in A+A$. To show that $A+A$ is essentially degenerate (mod k), it suffices to show that $A+A$ contains all but finitely many of the nonnegative integers congruent to $r \pmod k$. Since the single residue class $r \pmod k$ is equal to the union of the g/k residue classes $(r+ik) \pmod g$, $0 \leqslant i \leqslant (g/k)-1$, we need only show that $A+A$ contains all but finitely many of the nonnegative integers congruent to $(r+ik) \pmod g$ for each i, $0 \leqslant i \leqslant (g/k)-1$. A is degenerate (mod g), hence $A+A$ is essentially degenerate (mod g), so it suffices to show there is at least one representative of each of the classes $(r+ik) \pmod g$.

Finally note that since $k \in H(\bar{A}+\bar{A})$, $k + \bar{A}+\bar{A} = \bar{A}+\bar{A}$, and so $ik + \bar{A}+\bar{A} = \bar{A}+\bar{A}$ for $0 \leqslant i \leqslant (g/k)-1$. Thus for each $r \in A+A$, $r+ik \pmod g$ is represented in $A+A$, which is the desired result.

LEMMA 3. *Let A and B be sum disjoint and degenerate* (mod g). *If $\bar{A}+\bar{A}$ is periodic* (mod g) *then there exists sequences A' and B' such that*

(i) *$\underline{d}(A) \leqslant \underline{d}(A')$ and $\underline{d}(B) \leqslant \underline{d}(B')$,*

(ii) *A' and B' are sum disjoint,*

(iii) *A' and B' are degenerate* (mod k) *for some positive integer k such that $k|g$ and $k < g$.*

Proof. Since $\bar{A}+\bar{A}$ is periodic (mod g), we have by Lemma 2 that there exists a positive integer k such that $k|g$ and $A+A$ is essentially degenerate $(\bmod k)$. Let A' be the union of the nonnegative residues $(\bmod k)$ for which there is a representative in A. Thus A' is degenerate $(\bmod k)$ and since $A \subset A'$ we have $\underline{d}(A) \leqslant \underline{d}(A')$.

Now assume $c \in (A'+A') \cap (B+B)$. Then there exists $a_1', a_2' \in A'$ and $b_1, b_2 \in B$ such that $c = a_1'+a_2' = b_1+b_2$. From the definition of A', there exists $a_1, a_2 \in A$ such that $a_1+a_2 \equiv b_1+b_2 \equiv c (\bmod k)$. Since $B+B$ is essentially degenerate $(\bmod g)$ and $k|g$, there are infinitely many solutions to $b_1'+b_2' \equiv c (\bmod k)$ with $b_1', b_2' \in B$. But $A+A$ contains all but a finite number of the positive integers congruent to $c (\bmod k)$. This contradicts the fact that A and B are sum disjoint. Hence, we must have that A' and B are sum disjoint and by Lemma 1 there exists a sequence B' with the desired properties.

Hence, by repeated applications of Lemma 3 we will, in a finite number of steps, obtain two sequences A and B which are sum disjoint, degenerate $\bmod g$, having densities at least as large as the original sequences, and such that neither $\bar{A}+\bar{A}$ nor $\bar{B}+\bar{B}$ is periodic.

THEOREM 3 (Kneser [3], [5]). *Let $\mathscr{A}$ and $\mathscr{B}$ be subsets of a finite abelian group G. If $\mathscr{A}+\mathscr{B}$ is not periodic then $[\mathscr{A}+\mathscr{B}] \geqslant [\mathscr{A}]+[\mathscr{B}]-1$.*

It follows from Theorem 3 that $[2\bar{A}] \geqslant 2[\bar{A}]-1$ and $[2\bar{B}] \geqslant 2[\bar{B}]-1$. Let $[\bar{A}] = r$ and $[\bar{B}] = s$ with $r \leqslant s$. If $g \geqslant 2r+2s-1$ it can be shown through elementary computation that Theorem 1 must hold.

If either $[2\bar{A}] \geqslant 2[\bar{A}] = 2r$ or $[2\bar{B}] \geqslant 2[\bar{B}] = 2s$ then $g \geqslant 2r+2s-1$. Thus we need only consider the case $[2\bar{A}] = 2r-1$ and $[2\bar{B}] = 2s-1$. Since $g \geqslant (2r-1)+(2s-1) = 2r+2s-2$, the proof will be complete once it is shown that $g = 2r+2s-2$ is impossible.

Suppose there is a counterexample to Theorem 1. Then there exists sequences A and B which satisfy all the above and what is more, we can choose them with a minimal g.

First we observe that $[\bar{A}-\bar{B}] \leqslant (g-2)/2 = r+s-2$. Since A and B are sum disjoint and degenerate $\bmod g$, it follows that $0 \notin \bar{A}-\bar{B}$, $g/2 \notin \bar{A}-\bar{B}$, and if $x \in \bar{A}-\bar{B}$ then $-x \notin \bar{A}-\bar{B}$.

Now, since $\bar{A}-\bar{B} = \bar{A}+(-\bar{B})$, by Theorem 3 $\bar{A}-\bar{B}$ is periodic. Thus there exists h, $h < g$, such that if $t \in \bar{A}-\bar{B}$ then $t+nh \in \bar{A}-\bar{B}$. Define

$$A' = \{n\colon\ n \equiv a (\bmod h) \text{ for some } a \in A\},$$

$$B' = \{n\colon\ n \equiv b (\bmod h) \text{ for some } b \in B\}.$$

Clearly A' and B' are degenerate $\bmod h$, $h < g$, and $d(A')+d(B') \geqslant d(A)+d(B)$. It suffices to show A' and B' are sum disjoint. If so, A' and B' will provide us with a new counterexample degenerate $\bmod h$ with $h < g$.

If A' and B' are not sum disjoint then there exists $a_1', a_2' \in A'$ and

$b_1', b_2' \in B'$ such that $a_1'+a_2' = b_1'+b_2'$. Thus there exist $a_1, a_2 \in A$, $b_1, b_2 \in B$ such that

$$a_1+n_1h+a_2+n_2h = b_1+m_1h+b_2+m_2h.$$

Thus for some n, $a_1+a_2 = b_1+b_2-nh$ or $\big((a_1-b_1)+nh\big)+a_2 = b_2$. By the periodicity of $\bar{A}-\bar{B}$ we have $(a_1-b_1)+nh = a_3-b_3$. Hence, $(a_3-b_3)+a_2 = b_2$ or $a_3+a_2 = b_2+b_3$, a contradiction since A and B are sum disjoint.

This completes the proof of Theorem 1.

As immediate consequences of Theorem 1 and its proof, we have the following:

COROLLARY 1.2. *If A and B are sum disjoint and $\underline{d}(A)+\underline{d}(B) = 2/3$ then there exists sequences A' and B' degenerate* (mod 3) *such that $A \subset A'$ and $B \subset B'$ and $A'-A$ and $B'-B$ are finite.*

COROLLARY 1.3. *If A and B are sum disjoint and there are no sequences A' g-worse than A, or B' g-worse than B, for any g, then $\underline{d}(A)+\underline{d}(B) \leqslant 1/2$.*

3. Higher order sums. It is natural to ask if there are analogous results to Theorem 1 for sums $kA = \{n\colon\ n = a_1+a_2+ \ldots +a_k,\ a_i \in A\}$. In this direction we have established the following:

THEOREM 4. *If A and B are sets of nonnegative integers and $kA \cap kB = \emptyset$ for $k = 1, 2, \ldots, h$, then $\underline{d}(A)+\underline{d}(B) \leqslant 2/(h+1)$.*

THEOREM 5. *If A and B are sets of nonnegative integers and $hA \cap hB = \emptyset$ then $\underline{d}(A)+\underline{d}(B) \leqslant 2/m$ where m is the smallest positive integer which does not divide h.*

It is easily seen that the bounds in Theorems 4 and 5 can be attained. In Theorem 4 take $A = \{n\colon\ n \equiv 0 (\bmod h+1)\}$, $B = \{n\colon\ n \equiv 1 (\bmod h+1)\}$. In Theorem 5 take $A = \{n\colon\ n \equiv 0 (\bmod m)\}$, $B = \{n\colon\ n \equiv 1 (\bmod m)\}$. Since $m \nmid h$, $h \not\equiv 0 (\bmod m)$.

Theorem 5 is easily proved once Theorem 4 is known. If $k|h$ and $kA \cap kB \neq \emptyset$ then clearly $hA \cap hB \neq \emptyset$. Therefore, by the definition of m in Theorem 5, $kA \cap kB = \emptyset$ for $k = 1, 2, \ldots, m-1$. Now apply Theorem 4.

The proof of Theorem 4 begins along the same lines as Theorem 1 with the appropriate modifications. The difference occurs after establishing the h-hold sum analogue of Lemma 3. Using the analogue of Lemma 3 and Theorem 2, one obtains two sequences A and B such that $kA \cap kB = \emptyset$ for $k = 1, 2, \ldots, h$ neither $h\bar{A}$ nor $h\bar{B}$ is periodic, and they are degenerate $(\bmod g)$ for some $g \leqslant 2(h+1)$. Examining the different cases yields the stated result.

References

[1] P. Erdős and A. Sárközy, *On differences and sums of integers, I*, Journ. Number Theory 10 (1978), pp. 430–450.

[2] H. Halberstam and K. F. Roth, *Sequences*, Vol. I, Oxford University Press, 1966.

[3] J. H. B. Kemperman, *On small sumsets in Abelian Groups*, Acta Math. 103 (1960), pp. 63–88.
[4] M. Kneser, *Abschätzung der asymptotischen Dichte von Summenmengen*, Math. Zeitschr. 58 (1953), pp. 459–484.
[5] — *Ein Satz über abelsche Gruppen mit Anwendungen auf die Geometrie der Zahlen*, ibid. 61 (1955), pp. 429–434.

Received on 3.3.1981
and in revised form on 6.4.1983 (1244)

ACTA ARITHMETICA
XLIV (1984)

Sommes de puissances et d'irréductibles dans $F_q[X]$

par

MIREILLE CAR (Marseille)

I. Introduction. Soit F_q le corps fini à q éléments. De nombreuses analogies entre l'arithmétique de l'anneau $F_q[X]$ des polynômes à une indéterminée sur le corps F_q et l'anneau Z des entiers relatifs ont été mises en évidence, notemment en ce qui concerne l'arithmétique additive. Les problèmes de Goldbach, [5], et de Waring, [2], [8], ont été étudiés, et plus particulièrement le problème de Waring pour les carrés. Il est actuellement connu que tout polynôme $M \in F_q[X]$, de degré assez élevé, est représentable comme somme de trois polynômes irréductibles de degré au plus égal au degré de M, [5], et que, tout polynôme de degré $2n$ ou $2n-1$ assez élevé, est représentable comme somme de trois carrés de polynômes de degré au plus n, [3]. Nous nous intéressons ici à la représentation d'un polynôme de $F_q[X]$ comme somme d'une puissance k-ième et de deux polynômes irréductibles. Ce problème a déjà été étudié dans [9] pour les polynômes de degré multiples de k. On y démontre le théorème suivant:

THÉORÈME. *Soit k un entier de l'intervalle $[2, p[$, où p est la caractéristique du corps F_q. Alors, si n est un entier suffisamment grand, tout polynôme $K \in F_q[X]$ de degré nk est représentable comme somme*

$$K = a_1 P_1 + a_2 P_2 + a_3 A^k,$$

P_1 et P_2 étant des polynômes irréductibles unitaires de degré nk, A étant un polynôme unitaire de degré n, a_1, a_2 et a_3 étant des éléments de F_q.

Il est possible d'avoir de telles représentations pour des polynômes de degré non multiple de k, et même d'avoir des représentations de la forme

$$K = P_1 + P_2 + A^k,$$

les polynômes P_1 et P_2 étant irréductibles, mais non nécessairement unitaires, A étant un polynôme, ces polynômes vérifiant de plus, des conditions de degré. On peut aussi exiger que le polynôme A intervenant dans une telle représentation soit irréductible. C'est ce qui est fait ici, où l'on démontre essentiellement le théorème suivant:

THÉORÈME. *Soit k un entier de l'intervalle $[2, p[$, où p est la*